CART SOME TO SECOND S

Project Convergence

Plus:

- Battery charging
- FA26
- Pearl Harbor Anniversary



Contents

3. Command Team

4.
Army assesses wins, challenges as Project Convergence 2021 experimentation comes to a close

7.
Army R&D energizes battery charging for Soldiers

9. Working as a Network Systems Engineer

11.80 years ago: the Signal Corps during the attack on Pearl Harbor

The Army Communicator is published as a command information epublication for the men and women of the United States Army Signal Corps under the provisions of AR 360-1.

Opinions expressed herein do not necessarily reflect the views of Office, Chief of Signal, the US Army or the Department of Defense.

Submit articles, photos, graphics, videos, story ideas, and nominations for "Signal Spotlight" to the editor <u>here</u>. For additional information, please call (706) 791-7384.

Follow the Signal Regiment on Facebook <u>here</u>.

Follow the Signal School Commandant on Twitter here.

COL James Turinetti IV Signal School Commandant

CSM Darien Lawshea Signal Corps Regimental Command Sergeant Major

CW5 Chris Westbrook Signal Corps Regimental Chief Warrant Officer

Nicholas M. Spinelli Editor-in-Chief

On the Cover

A US Army Paratrooper assigned to 1st Brigade Combat Team, 82nd Airborne Division talks into a radio microphone during an exercise. The 82nd Airborne participated in Project Convergence 21 at Yuma Proving Ground, Ariz., this fall to experiment with new technologies and tactics, including how the network supports integrating weapons systems and command and control systems and enables communications with the Joint Force.

Photo by Sgt. Justin Stafford

Signal Regimental Team

And just like that, we've wrapped another year. It's been an incredible 12 months, and we've accomplished so much. From the return of TechNet to the official launch of MOS Convergence Phase 1, 2021 has been a humongous success, not just for Signal, but for the entire Force.

One of those successes is the recently completed Project Convergence. Army teams worked alongside service counterparts for an extended period of workshopping and experimentation that will pave the way for advancements in communication and warfighting capabilities. Our team was able to see some of these proposed capabilities during a visit to the exercise, and I hope you're as excited as I am for what's to come.

This month, we also were able to witness the extraordinary talents of our communicators during one of the first full-scale division level tactical exercises in over two decades during a visit to the 101st Airborne Division. And, most recently, we saw the reactivation of the 22nd Corps Signal Brigade, I Corps' Signal Brigade, which activated on November 22. Responsible for the communications and information system support for mission command to an army corps, this activation supports the Army's focused force structure realignments.

Before we end, let's take a moment to focus on safety. December typically sees a drastic increase in accidents both at home and on the road, so we should all focus on staying vigilant. If you're travelling for the holidays, keep safety in mind. The weather has been erratic to say the least and if you're going to be on the road, be prepared for sudden changes in conditions. Make sure to plan your routes accordingly and give yourself plenty of rest before and after driving long distances. Driving while exhausted in just as dangerous as driving while intoxicated.

For many, the holiday season also brings an increased risk of depression. If you're stressed, worried, anxious, or even just feeling a little down, please don't hesitate to reach out. Resources are available both on post and throughout the area. Remember, you're never alone.

As we close out 2021, I want to thank you all for your continued dedication to the Regiment. We could not complete the mission without you! Have a wonderful Holiday Season and a very Happy New Year!

Pro Patria Vigilans!



COL James Turinetti IV Signal School Commandant



CSM Darien Lawshea Regimental CSM



CW5 Chris Westbrook Regimental CWO

Army assesses wins, challenges as PC21 experimentation comes to a close

Maureena Thompson Army Futures

Senior members of the Army gathered at Yuma Proving Ground, Arizona, on Nov. 9 to discuss preliminary outcomes of Project Convergence 2021 (PC21), a large-scale modernization experiment that brought together roughly 1,500 participants from across the Joint Force to field-test future warfighting capabilities.

The Army-led event, which took place over six weeks in October and November and included components at Yuma Proving Ground and White Sands Missile Range, New Mexico, represents the largest Joint Force experiment conducted in 15 years.

By leveraging the technical and operational expertise of participating Service members and civilians from the Army, Navy, Marine Corps, Air Force and Space Force, as well as tech and defense industry partners in attendance, Army leaders were able to evaluate the strengths of new military technologies and assess how to most effectively synch Joint tactical maneuvers.

"A lot of this is actually looking at how we use data, how we use software, how we use algorithms to better connect sensors to shooters," said the Honorable Christine E. Wormuth, Secretary of the Army. Wormuth highlighted that continuing to hone Joint network and assured positioning, navigation and timing/space capabilities will be essential in furthering Joint All-Domain Command and Control.

In simulating the speed and scale of a multi-domain

fight, PC21 illustrated the urgency of the U.S. military's shared focus on attaining the speed, range and convergence required for competitive overmatch. Strategic exercises conducted as part of the experiment enabled the Joint Force to pinpoint which integrated networks and maneuvers worked well and which could benefit from additional improvements.

PC21 organizers executed seven use cases to test



A US Army Paratrooper assigned to 1st Brigade Combat Team, 82nd Airborne Division talks into a radio microphone during an exercise. The 82nd Airborne participated in Project Convergence 21 at Yuma Proving Ground, Ariz., this fall to experiment with new technologies and tactics, including how the network supports integrating weapons systems and command and control systems and enables communications with the Joint Force.

Photo by Sqt. Justin Stafford

the interoperability of Army and Joint technologies during the event. The efforts resulted in a significant broadening of the command and control network, allowing for the expansion of operating ranges and greater battle-field visibility.

Also taking center stage at PC21 were a number of groundbreaking prototypes that incorporated artificial intelligence, robotics and autonomy to increase precision and lethality while mitigating risks to combat troops. The innovative systems and tools — some still in early development and others at or near completion — will offer the Army additional operational options and flexibilities.

"This is about technology, but this is also about how we fight and how we restructure the Army for the future," explained Gen. John M. Murray, commanding general of Army Futures Command.

Many of the capabilities under development represent a shift away from focusing on counterinsurgency and counterterrorism and toward preparing for the possibility of large-scale conflict.

"We're at an inflection point," said Gen. James C. McConville, Chief of Staff of the Army. "In order to deter strategic competitors, we need to be able to do large-scale combat operations."

Such operations typically involve the use of longrange precision fires and land warfare, which is why the Army is prioritizing the development of hypersonic missiles, next-generation combat vehicles and other battleessential materiel.

"We're looking for edge, we're looking for advantage and we're doing it working together as a Joint Force," McConville said, adding that the Army is also "going to do it working together as a combined force with allies and partners" in the very near future.



Lt. Gen. James M. Richardson of Army Futures Command discusses the aims of Project Convergence during an AUSA 2021 Contemporary Military Forum.

Photo by Sgt. 1st Class Henry Gundacker

Army leaders emphasized that the ability to test out new capabilities "in the dirt" as a combined force provides helpful insights into the future operational environment.

"One of the things we've learned over multiple exercises and regular iteration is the value of interacting and understanding where there's friction points, where there's literal or figurative firewalls and how to break those down," said Brig. Gen. James P. Isenhower III, commander of the 1st Multi-Domain Task Force. "When

we do, we find we can move faster, we can transmit data faster, we can make decisions faster."

Maj. Gen. Christopher T. Donahue, commander of the 82nd Airborne Division, asserted that "the integrated tactical network is very robust, and it is living up to what we thought it would be."

While the consensus was that the experiment produced promising results, Army leaders also acknowledged that budget constraints could influence the speed at which new technologies are rolled out across the points in informing new and continumilitary.

Despite these obstacles, leaders stressed that the Army's modernization efforts are ongoing and extend beyond capstone events such as PC21. Karen Saunders, senior official performing the duties of the Assistant

Secretary of the Army for Acquisition, Logistics and Technology, underscored the value of Soldier touching acquisitions; "We're refining the requirements all year long," she said.

"We're getting quality systems into the hands of Soldiers at the speed of relevance." added McConville.

Army leaders also detailed mission-critical plans to incorporate new capabilities into enduring systems and programs of record; more closely align acquisition processes across the Services; modernize legacy logistics procedures; and reinvigorate and refine talent management procedures.

As Army and Joint Force officials continue to analyze data and consolidate observations and lessons learned from PC21, they are also commencing planning for Project Convergence 2022, which will further hone modernization advancements and include the participation of allied partners.

"The United States Army will never fight by itself," Murray stated, explaining that the integration of Joint and allied force efforts will result in a stronger, faster, more lethal combined force capable of delivering unrivaled deterrence and overmatch.



Pvt. 1st Class Benjamin Sargent, assigned to 82nd Airborne Division, prepares a multi-mission payload Unmanned Aerial System for launch during Project Convergence at Yuma Proving Grounds, Ariz.

Photo by Sgt. Marita Schwab

Army R&D energizes battery charging for Soldiers

Dan Lafontaine **DEVCOM C5ISR**

Army researchers are exploring new ways to keep Soldiers' electronic devices powered during extended missions by using wearable fuel cells for on-the-move battery charging.

As the Army continues to modernize the force with high-tech Soldier-worn and handheld equipment like radios, GPS, night-vision devices and weapons, the energy demand is continually increasing.

ty and efficiency of emerging fuel-cell based power generation technology when operated with packaged fuels as well as commonly available substitutes such as windshield washer fluid.

Army Futures Command (AFC) is leading work on the Soldier Wearable Power Generator (SWPG) that enables on-the-move charging, thus reducing the number of batteries required to be carried.

"We're aiming to deliver a simple, easy-to-use way for Soldiers to extend battery life and keep moving in the field by developing wearable fuel cells," said Shailesh Shah, a chemical engineer with the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center — a component of AFC's Combat Capabilities Development Command (DEVCOM). "Enabling fuel cell operation on windshield washer fluid already in the Army's supply chain avoids the need to set up a logistics resupply of custom fuels. The SWPG simultaneously reduces dependence on logistics for battery resupply."

The C5ISR Center's research aligns with the Army's renewed emphasis and interest in fuel-cell power generation for supplying power to dismounted Soldiers, according to Shah. Technology in the industry has improved significantly in the past 10 years in terms of size, weight, noise, thermal signature reduction, improved modularity and mounting systems.

Adding wearable fuel cells to the Soldier system enables users to charge the currently fielded thin, flexible Conformal Wearable Battery (CWB) worn on vests as a Engineers are working on optimizing the power densi- central power source for electronic devices. The fuel-cell



Army C5ISR Center enlisted advisers Sqt. Corey Burrell (right) and Sqt. 1st Class Patrick Huggins demonstrate the Soldier Wearable Power Generator at Aberdeen Proving Ground, Maryland. Photo by Dan Lafontaine

research complements the C5ISR Center's concurrent work to modernize the CWB with advanced materials.

Researchers are continuing SWPG design modifications to improve performance of the prototypes with an emphasis on size and weight reductions, according to Christopher Hurley, chief of the Center's Tactical Power Branch. Soldiers on 72-hour missions could save 12 pounds in battery weight under normal power draws with current prototypes.

Additional organizations providing support are the Army's Project Manager Integrated Visual Augmentation System, DEVCOM Soldier Center, the FBI and the National Defense Center for Energy and Environment.

"A key to enhancing our fuel-cell development is placing different prototypes in the hands of Soldiers during field exercises," Hurley said. "C5ISR Center engineers have been side-by-side with Soldiers to gain feedback during the Army Expeditionary Warrior Experiment in 2020 and 2021 with plans for 2022. The Soldier touch points are an invaluable resource in our development process so we can immediately turn around and incorporate their evaluations into our hardware systems."



Soldier Wearable Power Generator Photo by Dan Lafontaine

Working as a Network Systems Engineer

Cpt. Andrew P. Zitter A Company, 741st Military Intelligence Battalion

As a 26A Network Systems Engineer, I design, build, and maintain reliable, available, and secure network solutions that enable Soldiers to share information to support winning the Nation's wars. There are over three hundred 26A's across all components of the Army, serving in positions at the tactical, operational, and strategic levels around the world. We lead small teams of highly specialized Soldiers, Civilians, and Contractors to solve complex and constantly evolving problems.

Every network engineer enters the career field This is a significant through the Voluntary Transfer Incentive Program (VTIP). a mechanic changi We are all infantrymen, artillerymen, aviators, signaleers, down the highway.



Courtesy image

and others that have firsthand experience with how Soldiers rely on their tactical and strategic networks. Armed with that knowledge, we are in the unique position to anticipate the needs of units and advocate on their behalf to design and build the solutions that they need in order to accomplish their mission.

As a junior captain, my first assignment was at the Regional Cyber Center at Camp Walker, South Korea. I lead and worked alongside a small team of Soldiers and DA Civilians responsible for operating, maintaining, securing, and upgrading the network infrastructure that enables communication to and from the Korean peninsula. This is a significant challenge in and of itself – sort of like a mechanic changing a tire on a car while it's speeding down the highway.

Network engineers are both planners and implementers; out-of-the-box thinkers that seek out and solve problems. I saw an opportunity to automate time-consuming and repetitive tasks that my team was responsible for. With the support of my leadership team, I worked with U.S. Army Pacific and my peers at the Regional Cyber Center in Hawaii to co-author a computer program that updated our security posture as new threats were identified and reported. This automation resulted in significant time, cost, and even energy savings for the Army.

Collaborating with engineers and technicians in other organizations across South Korea, I also worked on enhancing integration of tactical systems into the country-wide strategic backbone. As one team, we developed a solution that would enable a unit to deploy anywhere in the country, connect to the strategic network using whatever equipment was available to them, and immediately

organizations.

around the world, South Korea was in close proximity to the source and was impacted earlier than most Western countries. Reeling from new lockdown orders, my team and I rapidly coordinated with our customers,

and securely communicate with other designing, securing funding, and ultimately building the upgraded infra-When COVID-19 began spreading structure that enabled United States Forces Korea (USFK), 8th Army, and all other units to telework safely and securely.

This career field offers experiences that few in the Army get to be a part of and is filled with extremely talented people. We are constantly engaged; every position we serve in is Key Developmental.

If leading a team of subject matter experts, developing creative solutions to complex problems, and making a big impact on the Army sounds appealing, then network engineering might be for you.



Courtesy image



80 years ago: the Signal Corps during the attack on Pearl Harbor

Steven J. Rauch Signal Corps Branch Historian

Vulnerability. A word well known to all Signaleers who install, operate, maintain and defend the cyberspace domain. Recognizing a threat, identifying the target of the threat, and reducing or eliminating the vulnerability of the target through implementation of defensive measures seems logical and even simple on the surface. However, as Clausewitz said in his book *Vom Krieg*, "Everything in war is very simple, but the simplest thing is difficult." One also has to be careful during the process of protecting an asset from one type of threat to not open up a vulnerability and expose other assets to attack from other types of threats. But can everything be defended? If not, what is the priority to mitigate potential damage from an enemy attack though not entirely stop it? Even knowing specific information about enemy intent and potential action is often insufficient and in some cases may lead to wrong prioritizations regarding defensive measures and risk to important assets. Military history is replete with examples of how in spite of doing what was considered appropriate can lead to a disaster and the question "How did that happen?" Perhaps the most famous example of this dilemma was the multi-domain battle that occurred on December 7, 1941 when the Japanese Empire attacked US military forces and bases in the Hawaii Islands on that fateful day.

During events leading up to and during the attack soldiers of the Signal Corps had to overcome numerous challenges to provide communications at all levels of war US Army Hawaiian Department
7 December 1941

Signal Corps Units, Strength, and Supported Units

Ft. Shafter • 9th Signal Service Company - Department/Garrison Operations	Enlisted 327	Officer 1
Hickam Field • 12 th Signal Platoon (Air Base) - 17 th Air Base Group • 324 th Signal Company (Aviation) - 18 th Bomb Wing • 407 th Signal Company (Aviation) - detachments at Wake and Midway • 428 th Signal Company (Aviation)	27 73 72 73	1 4 3 3
Schofield Barracks • 24 th Signal Company - 24 th Infantry Division • 25 th Signal Company - 25 th Infantry Division • Signal Company (Air Warning) - SCR 270/271 Radar sites	133 136 348	4 5 13
Wheeler Field • 45 th Signal Platoon (Air Base) - 18 th Airbase Group • 307 th Signal Company (Aviation) - 14 th Pursuit Wing	23 <u>71</u>	1 3
TOTAL STRENGT	H 1,283	38

Source: Thompson, et.al. *The Signal Corps: The Test*, p. 7
Signal organizations in Hawaii – December 1941.
Chart by Steven J. Rauch.

from strategic to tactical. Some stories are well known, such as the radar warning that was not heeded. However, other lesser-known events provide lessons about overcoming the challenges of friction, chance and misunderstanding that may be worth considering during this 80th anniversary year.

From a strategic perspective, US forces in Hawaii increased in importance when President Roosevelt ordered the Navy in 1940 to move the Pacific Fleet from the US west coast to Pearl Harbor at Oahu. This was viewed by some as a way to deter Japanese aggression but others saw it as making the fleet more vulnerable to attack. Strategic communications therefore needed to be capable of reaching beyond the US mainland for effective command and control.

Prior to WWII the Signal Corps sought to modernize its strategic communications systems but often met resistance due to cost and other priorities. In 1939, the Signal Corps sought to expand the War Department Radio Network transmission facilities at Ft. Myer, VA with a rhombic antenna for point-to-point communications with Seattle, WA. However, the Ft. Myer garrison commander, Colonel George S. Patton, Jr., objected to the new antenna because it would encroach upon the polo field that was used for cavalry training so he blocked the modernization plan. When the US Navy offered the Signal Corps suitable buildings in Arlington, Patton again intervened because he enlisted soldiers. The Navy withdrew its offer and the Signal Corps was not cisco and Honolulu rendered existing able to modernize and expand its

transmission capabilities to the west coast or even to Hawaii thus creating a dormant strategic communications vulnerability that would be revealed years later. On the morning of December 7, 1941 Army Chief of Staff, George C.

Marshall was informed the Japanese government had broken diplomatic relations with the United States. He decided to send a warning of possible attack to Lt. Gen. Walter C. Short, commander of army forces in Hawaii. Though he could have used a special "scrambler" telephone, the information was deemed too important to risk verbal compromise so instead he sent an encrypted telegraph message through the War Department wanted those same facilities to house Radio Network. However, atmospheric disturbances near both San Fran-Army strategic communications circuits ineffective, something the expansion of radio facilities at Ft. Myer was intended to prevent. Therefore, Lt. Col. Edward F. French, OIC of the message center, had to quickly adapt

> French sent Marshall's message at 0647 Hawaiian time and told West-

and resort to commercial means

waii.

through Western Union to San Francisco and the Radio Corporation of America (RCA) to transmit it to Ha-



Men of the 9th Signal Service Company in Hawaii 1939. Signal Corps Historical Collection

ern Union he wanted an immediate report about its delivery. The RCA office in Honolulu received the message at 0733, twenty-two minutes be- from closing a large vulnerability in fore the attack and if a planned installation of new teletype connections to Fort Shafter had been completed, things may have been fine. Instead, a motorcycle messenger was told to deliver Marshall's message by hand to Ft. Shafter. While the messenger was enroute to Ft. Shafter, the enemy attack began and caused chaos and traffic jams on the roads. At 1145, the courier arrived at the Ft. Shafter message center. Signal personnel then had to process the message through the cipher machine and that took another hour or so. The message made it to General Short's aide at 1458 and he handed it to Short at 1500. So because of a series of decisions that took place years before the event, a simple message got through, but it took eight hours and 13 minutes to arrive after being sent and more importantly, seven hours and five minutes after the attack had occurred.

What lessons regarding strategic communications vulnerability might be gleaned from this episode? Priorities for one. Pre-war competition within the Army for limited resources. such as military real estate, had a

profound impact on strategic communications capability. Local priorities at Ft. Myer prevented the Signal Corps strategic communications capabilities that hindered the ability to get timely information into the hands of commanders who needed it halfway around the world

On December 7, 1941, the Signal Corps contingent in the Hawaiian Department consisted of 38 officers and 1,283 enlisted men. The department Signal Officer, or G6, was Lt. Col. Carroll A. Powell. The Hawaiian Department G6 office was responsible for the installation, operation, and maintenance of communications to all Army camps, posts, and stations in the Hawaiian Islands. Because the army included the Army Air Corps. the Signal Corps was responsible for the communications missions for that element, including airfield communications and operational units. Of these units, the largest was the Signal Aircraft Warning Company with 361 personnel assigned to operate the top-secret radar sets being deployed in Hawaii.

The Army had established extensive coastal defenses throughout the islands to engage an enemy approaching from the sea or air. Army long-range artillery batteries; anti-



SCR 270 Mobile Radar Set of the type employed on Oahu at the time of the battle. Signal Corps Historical Collection.

aircraft artillery batteries; Army Air Corps airfields; radar installations, and support facilities were all connected through a Signal Corps fire control command and communications system using subterranean telephone cables throughout the islands. With this cable system, the Hawaiian Department could communicate sightings of enemy vessels or aircraft along with range plotting data needed to engage them.

However, on December 7 this system was not operational because the Corps of Engineers was in the process of upgrading and remodeling the communications tunnels, a heavy construction project that involved explosives and excavating equipment that caused shaking and vibrations.

To avoid damage to scarce equipment, the telephone switchboards and distribution cables had been removed to protect them from the engineer's activities. As a result, the Hawaiian Department command post was without telephone capability that morning. However, once the enemy attack began, 1st Lt. William Scandrett, the wire construction officer, along with Warrant Officer John E. Carney quickly gathered their crews at the command post and restored communications before the enemy attack was over.

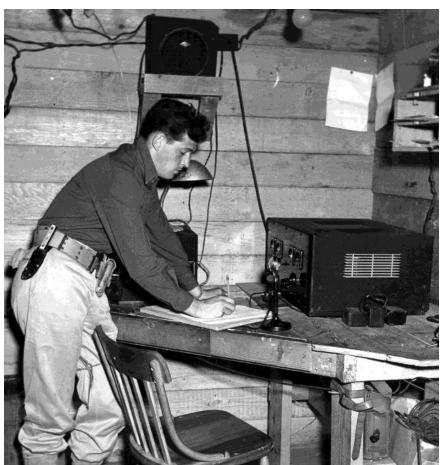
The most famous of event of this day involves the Signaleers who operated the top-secret aircraft warning

> radar units. These systems were still experimental and still in a training status. A training schedule developed by the Army Interceptor Command called for the radar sets to operate only 3 hours each day, from 0400 - 0700 hours. The limited schedule was designed in part to prevent burning out the big hot electron tubes and conserve limited replacement parts. In addition, because the sabotage threat was deemed most likely, an air atcern.

> On that morning two signalmen, Privates George A. Elliott

and Joseph L. Lockard, were operating a mobile SCR 270B at Opana at Kuhuku Point on the northern tip of Oahu. At 0700, they prepared to end their duty and close down the radar system, but since the truck had not arrived to take them, back to camp they used the time to continue training on the system. At 0702, a large echo appeared on the oscilloscope that seemed out of the ordinary. After checking the system to make sure it was working properly, Elliott and Lockard determined the echo was indicating a large flight of aircraft about 132 miles away approaching from the north at a speed of about 3 miles a minute.

Elliott suggested to Lockard that they should report it to the information center, so at 0720 Elliott called Ft. Shafter. Ironically, the information center had been full of Air Corps and Naval aircraft trackers until 0700 when all of them promptly departed at the end of their shift. Elliott gave the information to Pvt. Joseph P. McDonald who thought he was the only one in the building until he saw a Ione Army pilot, Lt. Kermit Tyler who tack was less of a con- had been assigned to a four-hour shift in order to become acquainted with the routine. It was therefore an accident that two men at Opana and two men at the air-warning center



Pvt. Joseph Lockhart who detected the Japanese planes approach at 0702 hours December 7, 1941. Signal Corps Historical Collection.

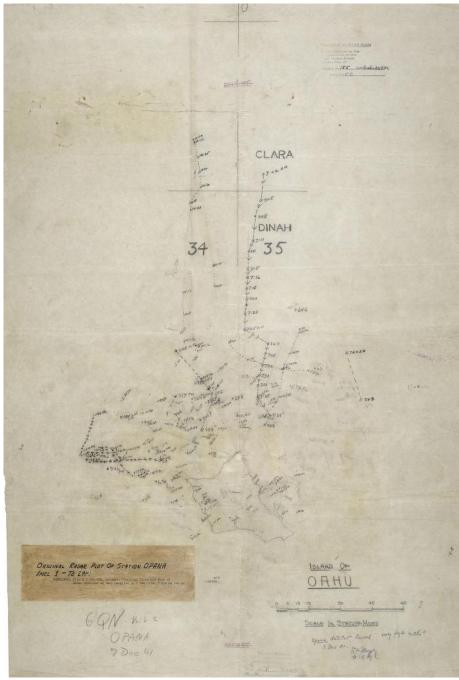


Image of original radar plot showing time and distance of Japanese planes as they approached Oahu.
Signal Corps Historical Collection.

were present and aware of critical information within minutes of the attack. McDonald told Tyler about the message but Tyler showed no interest. McDonald called Opana back and this time a very excited Lockard insisted on speaking to someone in charge. Tyler got on the line and in so many words told Lockard to forget about what he was seeing because there was a flight of B-17 bombers arriving early that morning and they were probably causing the echo. Back at Opana. Lockard and Elliott followed the blip until it disappeared due to the surrounding mountains. At 0739, the truck arrived to take them back to camp for breakfast. The Japanese planes struck Pearl Harbor at 0755.

What lessons regarding operational vulnerability can be taken from these two episodes? The engineers needed to improve and modernize the communications tunnels, however disconnecting telephone services to the Hawaiian De-

partment command post opened a vulnerability, even if temporary, that hindered the ability to respond to the attack. Signal soldiers quickly restored communications and eliminated the vulnerability so the commanders could exercise control. The story of radar detecting the impending attack illustrates how concern for wear and tear on equipment created a significant vulnerability by operating the systems only three hours each day. What about the other 21 hours? At 0700, all radar was to be turned off to avoid overheating and consumption of spare parts. However, by sheer luck, the Opana radar was still operating at 0702. but the nerve center for analyzing and acting upon such information had shut down at 0700. Only by chance were two men still in the information center and neither of them were in a position to understand or act upon the information that had been acquired by new technology and diligent equipment operators. This vulnerability was

power became focused on interception operations.

Many challenges at the tactical level were driven by the defensive measures against sabotage. For example, the 98th Antiaircraft Regiment at Schofield Barracks had removed all of their telephones and switchboards from the anti-aircraft gun positions and locked them in the supply room to protect against that threat. However, having communications equipment locked up in a central location instead of dispersed where it was needed created a command and control gap for critical air defense systems. During the attack, the regimental communications section guickly set up the switchboards and connected telephones to the gun positions and command post. This was done in spite of danger from enemy aircraft who strafed ground positions. About 0830 that morning, 2nd Lt. Stephen G. Salzman and Staff Sgt. Lowell V. Klatt saw two Japanese planes line up to attack them as they worked at restoring communications to a gun position so they had pause and use their rifles to shoot at the aircraft. One of the planes tried to avoid the fire, flew into high tension power wires and crashed behind the command post. Salzman and Klatt then

also quickly eliminated when all man- resumed their mission and within 25 minutes all communications equipment was connected even before the anti-aircraft guns, that had also been stored to protect against sabotage, were brought to their positions.

> What lessons regarding tactical communications vulnerability might be gleaned from this episode? Clearly, efforts to protect against the most likely threat instead of the most dangerous threat drove the command to remove not just communications equipment, but ammunition and systems to protected locations. This attempt to defend against the sabotage threat opened the unit up to the most dangerous threat – enemy air attack and though soldiers acted quickly to eliminate the vulnerability, the enemy needed only minutes to attack their targets.

As can be seen, vulnerabilities to communications capability extended from the strategic to the tactical. Some vulnerabilities had existed for years and some for a short amount of time. Nevertheless, all existed the day the Japanese attacked Hawaii. Pearl Harbor is a story of how individuals reacted that day. Senior command and control was paralyzed for a time, but at the soldier level, leaders and men attempted to fix what was wrong immediately. Scandrett's

crews restored the command post switchboards and phones as quickly as they could. Salzman and his men restored switchboards and telephones to the anti-aircraft guns before the guns could even be brought into position. Within a half an hour of the first enemy bomb, all six radar sites were operating and connected to the information center. Maybe the biggest lesson is getting the message through is important but can the information be in the decision makers hands when they need it to execute operations. That job is as important today as it was 80 years ago at Pearl Harbor.

PEARL HARBOR

DECEMBER 7, 1941, A DATE WHICH WILL LIVE IN INFAMY... NO MATTER HOW LONG IT MAY TAKE US TO OVERCOME THIS PREMEDITATED INVASION. THE AMERICAN PEOPLE, IN THEIR RIGHTEOUS MIGHT. WILL WIN THROUGH TO ABSOLUTE VICTORY.

Courtesy image

